REMARKS – General

Claim Rejections under 35 USC §112:

The most recent Office Action (OA) rejects claims 1-29 as being indefinite. Specifically, the OA states that there in insufficient antecedent basis for the limitation "the target device." Applicants have amended claim 1 (as well as claim 39) to recite –the target wireless device—. Applicants respectfully request reconsideration of the rejection.

Claim Rejections under 35 USC §101:

The OA rejects claims 30-33, 35-36, 39-44, and 61-73 as being directed towards non-statutory subject matter. Specifically, the OA states that claims 30 and 61 recite "computer software components" for manipulating data. The OA cites *In re Warmerdam*, 33 F.3d 1354, 1361 (Fed. Cir. 1994) as authority for this rejection. The OA submits that a "*data structure* not claimed as embodied in a computer-readable medium are descriptive material *per se* and are not statutory because they are not capable of causing a functional change in the computer." *Id.* Emphasis added. Applicants respectfully traverse this rejection.

Applicants respectfully submit that reliance on *Warmerdam* is misplaced in that the court in *Warmerdam* limited non-statutory subject matter to "data structures" only. The rejection in the OA appears to imply that the components of the network-based system, recited in Applicants' claim 30 for example, are data structures. Otherwise, they would not be subject to *Warmerdam*. However, *Warmerdam* expressly defines "data structures" as "*physical or logical relationship[s] among data elements*, designed to support specific data manipulation functions." *Id.* Emphasis added.

Turning now to Applicants' claim 30, physical or logical relationships among data elements are not recited. To the contrary, modules for a network-based system (Claim 30, preamble), suitable for server-based applications (Applicants' specification, page 9, lines 16-25), are claimed, those modules performing the functions of:

- determining whether pre-provisioned content corresponding to a requesting device exists and where pre-provisioned content exists;
- determining whether the pre-provisioned content is stored locally or with a trusted, third party application provider;
- retrieving an application from one of the group consisting of locally stored data repositories and trusted, third party application providers where pre-provisioned content exists, and otherwise from untrusted, third party hosts; and
- examining the application by a method selected from the group consisting of examining the application to detect malicious code, performing a class analysis of the application to verify that classes in the application conform to desired standards, applying application filters to the application

Applicants respectfully submit that these modules are not merely "physical or logical relationships among data." To the contrary, they are system components configured to perform a tangible result – the provisioning and delivery of applications to wireless devices. Thus, these functions are not data structures, as defined in *Warmerdam*.

Further, since *Warmerdam* was decided in 1994, the Federal Circuit has given additional guidance on what constitutes statutory subject matter under 35 USC §101. Specifically, the Federal Circuit distinguished *Warmerdam* in 1999 in *AT&T Corp. v. Excel Communs., Inc.* 172 F.3d 1352 (Fed. Cir. 1999). In *AT&T*, the Federal Circuit held that "[t]he Supreme Court has construed § 101 broadly, noting that Congress intended statutory subject matter to "include anything under the sun that is made by man." *See Diamond v. Chakrabarty*, 447 U.S. 303, 309, (1980); *see also Diamond v. Diehr*, 450 U.S. 175, 182, (1981). "There are only three categories of unpatentable subject matter: "laws of nature, natural phenomena, and abstract ideas." *See Diehr*, 450 U.S. at 185. "[T]he mere fact that a claimed invention involves inputting numbers, calculating numbers, outputting numbers, and storing numbers, in and of itself, would not render it nonstatutory subject matter, unless, of course, its operation does not produce a 'useful, concrete and tangible result.'" *Diehr*, 450 US at 1374.

MPEP §2106, also citing *State Street Bank v. Signature Financial Group*, states that a machine or system programmed with software "…admittedly produces a 'useful,

concrete, and tangible result.' *This renders it statutory subject matter...*" *State Street Bank & Trust Co. v. Signature Fin. Group, Inc.*, 149 F.3d 1368, 1374-75, (Fed. Cir. 1998), *cert. denied*, 119 S. Ct. 851 (1999). Emphasis added. In *State Street*, the court held that even in a "processing system there was patentable subject matter because the system takes data representing discrete dollar amounts through a series of mathematical calculations to determine a final share price - a useful, concrete, and tangible result." *Id.* at 1373.

Applicants respectfully submit that claim 30, as well as claim 61, are recite system based components that produce a useful, concrete, and tangible result, namely that of provisioning and delivery of content to wireless devices. While the OA submits that they are not "claimed as embodied in computer readable media," Applicant respectfully notes that in *AT&T*, the Federal Circuit held that claims not reciting physical limitations set forth in the patent are indeed statutory subject matter, and that contrary arguments reflect "a misunderstanding of our case law." *AT&T*, 172 F.3d at 1359. Where the claims at issue "are directed to a process in the first instance, a structural inquiry is unnecessary." *Id.* "[A]fter *Diehr* and *Chakrabarty*, the [physical limitation] test has little, if any, applicability to determining the presence of statutory subject matter." *Id., citing State Street*, 149 F.3d at 1374.

As Applicants' claimed invention in claims 30 and 61 of a network based system and a computer-based content delivery system, respectively, configured to provision and deliver content to a wireless device are not data structures as set forth in *Warmerdam*, and as they each provide a useful, concrete, and tangible result, Applicants respectfully submit that both claim 30 and 61, as well as the claims depending therefrom, are statutory subject matter. Applicants respectfully request reconsideration of the rejection in light of these comments.

Claim Rejections under 35 USC §103:

The most recent Office Action (OA) rejects claims 1-33, 35, 36, 39-51, 55, 56, 58, and 60-73 under 35 USC §103 as being unpatentable over Tso et al., US Pat. No. 6,088,803, hereinafter "Tso", in view of Subramaniam et al., US Pat. No. 6,640,302, hereinafter "Sub," further in view of Jamtgaard et al., US Pat. No. 6,430,624, herein after

"Jam." (Note that the OA lists Jam as having No. 6,430,324. However, Applicants presume that the number is 6,430,624, and respond accordingly.) Applicants respectfully traverse this rejection.

Applicants respectfully submit that the combination of Tso, Sub, and Jam both fails to teach all of Applicants' claimed limitations. Further, the combination teaches away from Applicants claimed invention.

In traversing the rejection, Applicants reply upon MPEP §2143.03, which states, "To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Applicants respectfully submit that the combination of Tso, Sub, and Jam fails to teach all of Applicants' claimed limitations. Specifically, the combination of references fails to teach the step of determining whether the pre-provisioned content is stored locally or with a trusted third party host, and where the pre-provisioned content is stored with the trusted third party host, retrieving the pre-provisioned content from the trusted third party host following the step of determining whether pre-provisioned content corresponding to the device exists, and delivering the content to a target device without further provisioning.

To begin, none of Tso, Sub, or Jam teaches determining whether the pre-provisioned content is stored locally or with a trusted third party host, and where the pre-provisioned content is stored with the trusted third party host, retrieving the pre-provisioned content from the trusted third party host and delivering it without additional provisioning. The OA submits that Tso teaches "determining whether pre-provisioned content corresponding to the target device exists" at col. 8, lines 2-25, and further teaches "where the pre-provisioned content exists, determine whether the pre-provisioned content is stored locally or with a trusted third party host" at col. 6, lines 41-55. The OA further submits that Tso teaches "where the pre-provisioned content is unavailable, selecting content from remotely stored, untrusted applications and provisioning the content for the target device at col. 7, lines 33-63, col. 8, lines 2-25, where the provisioning "comprises intercepting the content and inspecting the content, wherein the inspecting comprises at least one of examining the content to detect malicious code, determining whether the content contains banned code, and determining whether the content contains designated

API at col. 2, lines 37-67, col. 3, lines 2-10 and lines 55-67, and col. 5, lines 27-43. Applicants respectfully traverse this assertion.

The specification of Tso, as has been set forth before (by both previous Office Actions and by Applicants) and is set forth again below, expressly teaches away from retrieving pre-provisioned content from a remote, trusted, third party hosts in that Tso's disclosure teaches examination of all content, regardless of source. *Applicants respectfully note that the Examiner has stated this very conclusion in the record by acknowledging in prior Office Actions that Tso fails to teach the step of determining whether the pre-provisioned content is stored locally or with a trusted third party host*, and where the pre-provisioned content is stored with the trusted third party host, retrieving the pre-provisioned content from the trusted third party host and delivering the content without further provisioning. See, e.g., the Office Action of June 25, 2007, page 5. "The combination of Tso-Jiang *does not disclose determining whether the content is stored locally or with a trusted third party host*, and where the pre-provisioned content is stored with the trusted third party host, retrieving the content from the trusted third party host." Emphasis added.

As has been set forth in prior responses, in claim 1, Applicants teach a provisioning system that first checks whether "pre-provisioned" content exists. Where the pre-provisioned content exists, Applicants' invention then determines whether the pre-provisioned content is stored locally or with a trusted third party host. Where pre-provisioned content is stored with the trusted third party host, Applicants' claimed invention retrieves the pre-provisioned content from the trusted third party host, and provides the pre-provisioned content to the target wireless device. Where the pre-provisioned content is unavailable, Applicants' invention selects content from remotely stored, untrusted hosts and then provisions the content for the target wireless device, with the provisioning comprising intercepting the content and inspecting the content, wherein the inspecting comprises at least one of examining the content to detect malicious code, determining whether the content contains banned code, and determining whether the content contains designated API. Applicants' invention then verifies that the target wireless device supports execution of the content by comparing the device capabilities to

the content requirements, and then provides the verified and provisioned content to the target wireless device.

Turning now to Tso, the reference draws a hard and fast line on any provisioning done by inspecting HTML websites for malicious code or viruses. They are *always* scanned. They are sometimes not scanned twice, as when they have already been inspected and are stored in a local cache memory, but received code is *always* scanned. Tso expressly teaches this at col. 3, lines 2-5, by stating "Once the file is completely received, network device 4 invokes virus checker 5, which in turn performs its preconfigured virus scan processing with the requested file as input (Step 40)."

The only time that the virus checker of Tso is not invoked is when it has *already been invoked* and is stored in a local cache. In other words, when the web page has been downloaded, already inspected once, and is stored locally. This is expressly taught at col. 5, lines 1-6, where Tso states, "Referring now to FIG. 4, since virus checking can be a resource-intensive operation, checked files and/or results of checks may be advantageously stored in a cache storage 30 resident in, or coupled to, network device 4. Future requests for the same data object may then be serviced immediately without having to *recheck* the file." Emphasis added.

Thus, Tso teaches inspecting *any and all content* received from a third party source. While the OA cites Tso at col. 6, lines 41-55, col. 7, liens 33-63, and col. 8, lines 2-25 as teaching detecting whether pre-provisioned content exists with a trusted third party host or is stored locally, Applicants respectfully submit that this is not the case, as previous Office Actions have acknowledged. Tso can check to see if code has already been inspected and is stored locally. However, if any code is retrieved from *any third party, i.e., from any location other than local cache*, the virus checker will be invoked when the code is received. In the sections cited by the most recent OA, Tso expressly states that his system, in the various embodiments, "provid[es] the virus checking functionality as discussed above." Tso, col. 6, lines 45-50. Tso simply fails to teach any determining whether content exists with a trusted, third party host and, where it does, delivering the content as claimed by Applicants.

The most recent OA states "Tso does not disclose…retrieving the pre-provisioned content from the trusted third party host and providing the pre-provisioned content to the

target wireless device." The OA then submits that Sub does teach such a step at col 10, lines 50-60 and col. 5, lines 64-67. However, Sub *fails to teach any step of provisioning* by examining the content to detect malicious code, determining whether the content contains banned code, and determining whether the content contains designated API. Thus, the only provisioning step is provided by Tso, which inspects *everything* that comes in the door. Sub inspects nothing, and Tso inspects everything. If code has already been inspected by Tso, it may be stored in memory. Thus, the combination must inspect *everything received,* and then either deliver it or store it locally for future use.

The OA appears to suggest that the absence of any provisioning in Sub means that the combination of Sub and Tso would employ the inspection of Tso in some instances and the absence of inspection in other instances. The OA suggests that the absence of inspection, as taught by Sub would somehow be used when a trusted third party host is called upon, while the inspection of Tso would be used when an untrusted host is called upon. This is despite the fact that no checking for pre-provisioned code is taught by either Tso or Sub, as noted above. Applicants respectfully submit that there is simply no teaching for selective provisioning in the combination of Tso, Sub, and Jam without using Applicants' invention and impermissible hindsight.

Applicants respectfully submit that, without an express teaching to the contrary, the combination of Sub, Tso, and Jam must either employ the inspection of Tso or the lack of inspection of Sub. (Jam fails to teach inspection as well, as noted below.) Applicants respectfully note that any suggestion to the contrary must be set forth with a rational underpinning or teaching. In making the case for obviousness, the Examiner has the burden of establishing the case in a well-reasoned and articulate way. "To facilitate review, this analysis should be made explicit." *KSR International v. Teleflex, Inc.*, 550 US ____, 127 S. Ct. 1727, 14 (2007), citing *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; *instead, there must be some articulated reasoning with some rational underpinning* to support the legal conclusion of obviousness.") Emphasis added. This burden exists because "*a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.*" *KSR* at 14. Emphasis added.

As previous Office Actions have asserted, Tso fails to teach any determining of whether pre-provisioned content exists with a locally stored host or a remote, trusted, third party. Further, Tso fails to teach any application where code is retrieved from a third party and is not inspected. Sub fails to teach any inspection at all. Similarly, Jam fails to teach any inspection or provisioning. Applicants respectfully submit that the combination of Tso, Sub, and Jam therefore fails to teach all of Applicants' claimed limitations. Further, as the combination teaches inspecting *all content when initially received, regardless of source*, Applicants respectfully submit that the combination teaches away from Applicants' claimed invention. Applicants respectfully request reconsideration of the rejection in light of these comments.

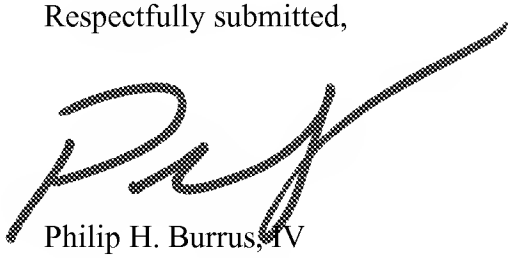
According to MPEP §2143.03, "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Applicants note also that claims 30, 45, and 61 have similar limitations as those recited in claim 1. As such, Applicants respectfully request reconsideration of claims 30, 45, 61 and their respective dependent claims 31-33, 35, 36, 39-44, 46-51, 55, 56, 58, 60, 62-73 in light of the comments above.

CONCLUSION

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless Applicant has argued herein that such amendment was made to distinguish over a particular reference or combination of references.

For the above reasons, Applicants believe the specification and claims are now in proper form, and that the claims all define patentably over the prior art. Applicants believe this application is now in condition for allowance, for which they respectfully submit. If any matter may be more easily handled by telephone, the undersigned attorney welcomes telephone calls from the Examiner.

Respectfully submitted,



Philip H. Burrus, IV
Attorney for Applicants
Registration No.: 45,432
404-797-8111
404-880-9912 (fax)